ENCLAVE
CHECKLIST V3R1.2

19 MAY 2006

Developed by DISA for the DOD

Database Reference Number: _____

Database entered by: _____ Date: _____

Technical Q/A by: _____Date: _____

Final Q/A by: _____ Date: _____

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

VMS 6.0 Enclave Procedures

AS01 Report

The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. In the section "Looking at Enclave Assets" is a quick step by step instruction in creating the report.

1. **Look at Enclave Assets**
   a. *Steps*
      i. Reports
      ii. AS01
      iii. Select Non-Computing (SUBMIT)
      iv. Select by Location (SUBMIT)
      v. Select the location
         1. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable.
      vi. Expand Non-Computing. - Expand Enclave – Expand the appropriate Enclave Type and check the box next to it.
      vii. Submit for Enclave Asset Report
      viii. View the following website for further details: https://vmscbt.disa.mil/index.htm
   b. *Problems*
      i. The element tree always starts at the top of a page. The element tree only prints for one page. If more data, it is truncated.

Performing the Review

If the Enclave asset is registered and under the correct location, skip to section titled First Review of the Asset. Ensure that the asset is registered in VMS under the correct organization.

1. **Creating/Registering the Asset**

   a. *Steps*
      i. Expand Asset Findings Maint
      ii. Expand Assets/Findings
      iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
      iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
      v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. Click the yellow folder icon located at the right of 'Non-Computing' to create an Asset.
vii. Click the General tab
- Enter the Enclave name (e.g., [Site_Name]_Enclave_Business_LAN) in "Display name" and add a Description
- Note: Use "Managed By" for remote locations being managed.
- Note: Use "Owner Field" to register asset to parent or child location.
- Note: Mac level, Confidentiality, & Use are defaulted. Change as required.

viii. Click the 'Asset Posture' tab to add postures to the asset:
- Expand Non-Computing
- Expand Enclave
- Choose the appropriate Enclave Type as defined by the Enclave STIG – Most will be General Business LAN Enclaves
- Click '>>' to move all selected options to the 'Selected' window
- Click on System/Enclave - Determine the enclave that the asset is part of. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen. For registered enclaves, choose the enclave. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
- Click 'Save'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

2. First Review of the Asset

If the asset is registered and it is the first time it has been reviewed, the following may need to be accomplished.

a. Steps

i. Expand Asset Findings Maint
ii. Expand Assets/Findings
iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. Expand 'Non-Computing'.
vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
viii. Click Asset name.
- Verify data in General tab and Asset Posture
- Click the 'Asset Posture' tab to add functions to the asset:
- Expand 'Non-Computing' in the 'Available' window
- Expand 'Enclave' in the 'Available' window
- Click the box associated with the correct Enclave Type
- Expand the asset in the 'Selected' window
- Click '>>' to move all selected options to the 'Selected' window
- Click on System/Enclave - Determine the enclave that the asset is part of. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen. For registered enclaves, choose the enclave. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
- Click 'Save'

ix. Continue with the following section 'Procedures for Review of the Asset' - Must Review'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

3. Procedures for Review of the Asset

If all registration tasks have been accomplished, use the following procedures:

a. Steps

i. Expand Asset Findings Maint
ii. Expand Assets/Findings
iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. Expand 'Non-Computing'.
vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
viii. Expand Asset to Review - When you drill down into the asset you will find Vulnerabilities assigned to the Enclave component.
ix. Expand a vulnerability
x. Update the 'Status' of the vulnerability
xi. Identify details on all open vulnerabilities

xii. If applicable: Apply to other assets by using the 'apply to other Findings' pane.

Note: Descriptions for Icons and Colors can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

4. Verify that all necessary assets were reviewed

a. Steps

i. Asset Findings Maint
ii. Visits
iii. Expand visit
iv. Expand location
v. Expand computing, non-computing, CNDS as applicable.
vi. Expand 'Must Review'
1. If checkmarks are gone, the asset has been reviewed or at a minimum has been opened and something has been changed on the asset.

ii. Reports
1. VC06 - Asset Compliance Report
2. Can select an asset or an org.
3. Select "open" status
4. Can sort on different fields
5. Display
a. Finding Comments
b. Finding Long Name
i. Because it is truncated otherwise
c. Finding Details
d. Vulnerability Discussion
6. VC03 Severity Summary Report
a. Has numbers only

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

5. Add Comments

a. Steps

i. Visit Maint
ii. Expand Organization the visit is set up for.
iii. Expand Visit
iv. Locate the visit you are working on.
v. Click on CCSD or enclave name.
vi. Comments Tab
vii. Save Changes

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

6. Compliance Monitoring

b. Steps

i. Reports
ii. VC06
iii. Can select an asset or an org.
iv. Select “open” status
v. Can sort on different fields
vi. Display
    1. Finding Comments
    2. Finding Long Name
        a. Because it’s truncated otherwise
    3. Finding Details
    4. Vulnerability Discussion
vii. VC03
    1. Has numbers only

Note: Additional information can be obtained in the VMS 6.0 WBT.
https://vmscbt.disa.mil/index.htm

EN010 V0003914 CAT II Enclave assets are not registered.

8500.2 IA Control: VIVM-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Enclave assets and/or systems that support enclave protection are not registered with an IAVM tracking mechanism (e.g., Vulnerability Management System (VMS)).

Checks

EN010

Interview the IAO and review the process to validate whether assets are registered in an IAVM tracking system. The Team Lead will review VMS to see if the system assets have been properly registered. Ask each reviewer if any assets were reviewed that were not in VMS or accurately identified in VMS.

Fixes

EN010

Register all enclave assests in a vulnerability management tracking system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN020 V0003915 CAT III SAs are not responsible for critical assets.

8500.2 IA Control: VIVM-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability System Administrators (SAs) are not responsible for critical assets or are not registered with a vulnerability management tracking system.

Checks

EN020

Interview the IAO and review the process to validate whether SAs are registered and responsible for critical assets. The Team Leader will check VMS to ensure that every asset has an assigned administrator. Team Leader will validate assignments but randomly selecting 4-6 administrators and interviewing them about their responsibilities. Compare VMS asset administrator assignments against the formal Assignments Letters.

Fixes

EN020

All SAs responsible for critical assests should register with VMS or an IAVM tracking system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN030 V0003916 CAT II IAVM notices are not responded to.

8500.2 IA Control: VIVM-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. E3.4.6.6 & E3.2.5.7

Vulnerability IAVM notices are not responded to within the specified period of time.

Checks

EN030

Ensure that the IAM has an established policy to ensure that IAVA notices are being acknowledged, implemented, and closed, in a timely manner. Ensure that System Administrators update affected systems in accordance with alert recommendations.

Fixes

EN030

The IAO and IAM, in coordination with the SA, will be responsible for ensuring that all IAVM notices are responded to within established guidelines.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN040 V0003917 CAT II Security related patches have not been applied.

8500.2 IA Control: VIVM-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para E3.2.5.7, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Security related patches have not been applied to all systems.

Checks

EN040

Interview the reviewers on the team to determine compliance and the IAO to determine if there is a patch process in place for the site. The reviewers will check for all security related patches on a device, either by manual or automated means.

Fixes

EN040

The IAO will ensure that all security related patches are applied. Some patches may be obtained from the DOD Patch Repository, otherwise contact the vendor.

The DOD Patch Repository can be accessed from the following URLs: https://patches.csd.disa.mil

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN041 V0004712 CAT II No documented security patch management process.

8500.2 IA Control: VIVM-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. E3.2.5.7, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A documented security patch management process is not in place or cannot be validated.

Checks

EN041

Interview the reviewers to determine compliance and the IAO to determine if there is a documented security patch management process in place for the site. The patch management process will ensure all security related patches are applied and that the process can be validated.

Fixes

EN041

Create a security patch management process that can be validated.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN042 V0004713 CAT III No automated patch distribution.

8500.2 IA Control: VIVM-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Workstations do not use an automated patch distribution process from a trusted site or secure source (i.e., tools such as Software Update Services (SUS), scripts, Tivoli, etc.) to distribute and apply security related patches.

Checks

EN042

Interview the IAO to determine if there is an automated patch distribution system for security related patches on workstations.

Each reviewer will report if each technology has a fully functional automated patch distribution solution. (Note: There is currently no DOD provided Unix solution.)

Fixes

EN042

The IAM will ensure workstations take advantage of technology and use an automated patch distribution process from a trusted site or secure source (i.e., tools such as SCRI, Windows Software Update Services (WSUS), scripts, Tivoli, etc.) to distribute and

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN043 V0007572 CAT III Patch testing is not performed.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Patch testing is not performed, prior to deployment, in a non-production environment.

Checks

EN043

Interview the IAM to determine if they have a policy in place that requires the testing of security patches, prior to deployment, in a non-production environment.

Fixes

EN043

The IAM will ensure testing of security patches is performed in a development or test environment (non-production environment) prior to deployment to production systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN043 V0007548 CAT III Patch testing is not performed.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Patch testing is not performed in a non-production environment.

Checks

EN043

Interview the IAM to determine if they have a policy in place that requires the testing of security patches in a non-production environment.

Fixes

EN043

The IAM will ensure testing of security patches is performed in a development or test environment (non-production environment) prior to deployment to production systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN050 V0003920 CAT III INFOCON procedures are not followed.

8500.2 IA Control: VIIR-1, VIIR-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability INFOCON procedures are not followed in accordance with Strategic Command Directive SD 527-1, 27 January 2006.

Checks

EN050

Interview the IAO to determine if they have an INFOCON policy in place and that INFOCON procedures are being implemented.

Fixes

EN050

The IAO will ensure compliance with INFOCON procedures in accordance with the Strategic Command Directive SD 527-1 dated 27 Jan 2006.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN070 V0003921 CAT III Supplemental SA INFOCON procedures not available.

8500.2 IA Control: VIIR-1, VIIR-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Supplemental SA INFOCON procedures are not available as required.

Checks

EN070

Interview the IAO to determine if they have an INFOCON policy in place and if they have supplemental SA instructions associated with the INFOCON policy.

Fixes

EN070

The IAM will develop and maintain supplemental procedures for use by the SAs as required, in consonance with INFOCON guidance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN080 V0003922 CAT IV EAL and robustness not adequate for systems.

8500.2 IA Control: DCSR-3, DCSR-2, DCSR-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para E3.2.5, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability IA or IA enabled products do not meet the minimum EAL and robustness level requirements as established by the Designated Approving Authority (DAA).

Checks

EN080

Interview the IAO to determine if they have a procurement policy in place that details IA requirements and incorporates NSTISSP 11 requirements.

Fixes

EN080

The IAO will ensure that all IA or IA enabled products meet the minimum EAL and robustness level requirements as established by the DAA.

Additional information on Common Criteria, a listing of validated products or products in evaluation, as well as pr

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN090 V0003923 CAT IV NSTISSP 11 not being followed for acquisition.

8500.2 IA Control: DCAS-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The acquisition of IA or IA-enabled products does not meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2.

Checks

EN090

Interview the IAM to determine if they have a procurement policy in place that details IA requirements.

Fixes

EN090

The IAO will ensure that the acquisition of IA or IA-enabled products meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN100 V0003924 CAT III Enclave assets are not assigned a MAC.

8500.2 IA Control: DCSD-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.7

Vulnerability Enclave assets are not assigned a Mission Assurance Category (MAC) or not assigned the correct MAC.

Checks

EN100

View VMS or interview IAO to determine if all assets, to include the enclave and the network, are assigned a Mission Assurance Category.

Fixes

EN100

The IAM will ensure all DOD information systems and enclaves are assigned a mission category directly associated with the importance of the information they contain relative to the achievement of DOD goals and objectives, particularly the warfighter's com

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN110 V0003925 CAT II Training and certification plan is not in use.

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The DOD component has not developed or implemented security training and certification plans and procedures.

Checks

EN110

Work with the Traditional reviewer to determine compliance and interview the IAO and ask them to provide the IA training and certification documentation.

Fixes

EN110

The IAM will ensure that the DOD component develops and implements training and certification plans and procedures for all personnel who use DOD computer systems to include Certifiers and Managers of Information Systems. Reference DODD 8570.1.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN120 V0003926 CAT III No established security features training program.

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability There is not a comprehensive user security features training program to include password and Internet usage guidance.

Checks

EN120

Work with the traditional reviewer to determine compliance and interview the IAM/IAO and ask to see the policy or documentation on security features (Internet usage, email usage, etc.) training requirements for all users.

Fixes

EN120

The IAM/IAO will establish and implement a comprehensive user security features training program to include password and Internet usage guidance (e.g. Security Features Users Guide or Standard Operating Procedure).

Requirements for formal and awareness

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN130 V0003987 CAT II No training of privileged users available.

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Training and certification of privileged users (SAs), IAOs, and other professional or management security personnel, is not provided or available.

Checks

EN130

Work with the traditional reviewer to determine compliance and interview the IAO to determine if there is a documented certification and training plan implemented for all privileged users and IA professionals.

Fixes

EN130

The IAM will provide training and certification for all privileged users (i.e. SAs and network administrators), as well as for all IAOs and other security personnel based on DOD and DISA SA standards for certification.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN140 V0003988 CAT II Need-to Know policy is not followed.

8500.2 IA Control: ECLP-1, ECAN-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.1.2.2, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Privileged users and IAOs have access to data, control information, software, and hardware for which they are not authorized access and do not have a need-to-know.

Checks

EN140

Work with all reviewers to determine compliance. Interview the IAO to determine if documentation/policy exists to enforce least privilege and need to know principles.

Fixes

EN140

The IAM will ensure that privileged users and IAOs access only that data, control information, software, and hardware for which they are authorized access and have a need-to-know.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN150 V0003989 CAT II No discretionary or role based access controls.

8500.2 IA Control: ECAN-1, ECPA-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para E3.4.7, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Demonstrated need to know and discretionary or role based access controls are not established.

Checks

EN150

Interview the IAO to determine if there is a process or procedure in place to determine a demonstrated need-to-know for access to DOD information. The process or policy must ensure that discretionary or role-based access controls are established and enforced, via operating system controls and access authorization forms, by the Information Owner. The IAO/IAM must enforce the establishment and use of RBAC and discretionary access controls.

Fixes

EN150

The IAM/IAO will ensure users have a validated or demonstrated need-to-know to access information, and discretionary or role-based access controls will be established and enforced, via operating system controls and access authorization forms, by the Infor

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN160 V0003990 CAT II Documentation of need-to-know is not available.

8500.2 IA Control: PRNK-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Documentation of need-to-know (e.g. DD Form 2875 or similar access form) is not available, does not exist, or is incomplete for individuals with access to a DOD network.

Checks

EN160

Work with the traditional reviewer to determine compliance and interview the IAO to determine if there is a policy in place to require system access forms for all users.

Fixes

EN160

The IAM/IAO will ensure all individuals with access to a DOD system or network require the following in the form of a DD Form 2875 or similar access authentication form:

- Verification of the users security clearance and/or investigative requirement fo

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN170 V0003991 CAT II Not compliant with DOD personnel requirements.

8500.2 IA Control: PRAS-2, PRAS-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Department of Defense (DOD) Directive 8500.1, Information Assurance Para. 4.8, Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. E3.2.1.8 and E3.4.8

Vulnerability Personnel authorization and investigation requirements are not in accordance with the DODI 8500.2.

Checks

EN170

Work with the traditional reviewer to determine compliance. Interview the IAO to ensure compliance with the DOD 8500.2 and DOD 5200.1-R requiements for personnel security.

Fixes

EN170

The IAM/IAO will ensure personnel authorization and investigation requirements are processed in accordance with DODI 8500.2

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN180 V0003992 CAT II Physical access is not controlled.

8500.2 IA Control: PECF-1, PECF-2

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.10.1 and 5.1.2.1, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Physical access is not controlled or limited to personnel with appropriate clearances.

Checks

EN180

Work with the Traditional reviewer to determine compliance. Interview the IAO to determine if there is a policy and procedure in place to prohibit unauthorized personnel from gaining access to DOD controlled areas.

Fixes

EN180

The IAO will ensure only authorized personnel with appropriate clearances are granted physical access to DOD computing facilities.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN190 V0003993 CAT III Not compliant with Traditional Security Checklist.

8500.2 IA Control: ECSC-1

References: Department of Defense (DOD) Directive 8500.1, Information Assurance Para. 4.8, Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.7.1.2 and 5.7.11, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Physical and/or environmental controls have not been established in accordance with DOD policy. The the site is not compliant with requirements contained in the Traditional Security Checklist.

Checks

EN190

Work with the Tradional reviewer to determine compliance. Interview the IAO to determine if there is procedure in place to follow DOD policy and regulations such as the DOD 5200.1-R, 5200.2-R, and the DODI 8500.2 in regards to environmental and physical security.

Fixes

EN190

The IAO will ensure all physical and/or environmental controls are established in accordance with DOD 8500.2, 5200.1-R Information Security Program, and the 5200.2-R Personnel Security Program.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN200 V0003994 CAT II No destruction of classified media procedures.

8500.2 IA Control: PECS-2, PECS-1, PEDD-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Procedures are not in place for clearing, sanitization or destruction of classified media.

Checks

EN200

Work with the traditional reviewer to determine compliance. Interview the IAO to determine if there are procedures in place for the destruction, sanitization, and clearance of classified media, devices, and data.

Fixes

EN200

The IAO will ensure procedures are in place for the removal or destruction of data by clearing, sanitizing, or destroying of classified media or equipment, prior to release outside of the security domain.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN210 V0003995 CAT II COOP or disaster recovery plans not exercised.

8500.2 IA Control: COED-1, COED-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability COOP or disaster recovery plans are not exercised in accordance with the MAC level of the system or network.

Checks

EN210

Interview the IAO to determine if a process is in place to exercise COOP and disaster recovery plans in accordance with MAC level requirements.

This check does NOT apply to Compliance Validation Visits.

Fixes

EN210

The IAM will ensure that the continuity of operations (COOP) or disaster recovery plans or significant portions are exercised in accordance with the requirements set forth in the DODI 8500.2 for the appropriate MAC level of the systems.

COED-2 - COOP,

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN220 V0003996 CAT II A disaster recovery plan does not exist.

8500.2 IA Control: CODP-2, CODP-1, CODP-3

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A disaster recovery plan does not exist.

Checks

EN220

Interview the IAO and ask to see the Disaster Recovery Plan that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level.

Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.

This check does NOT apply to Compliance Validation Visits.

Fixes

EN220

The IAM will ensure a disaster plan exists that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level. (Disaster recovery procedures include business recovery plans, system conti

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN230 V0003997 CAT II Critical systems are not backed up.

8500.2 IA Control: COBR-1, COSW-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Critical systems are not backed up and/or copies of the OS and other critical software are not stored appropriately.

Checks

EN230

Interview the IAO to determine if there is a backup policy in place to ensure backup of critical systems and that backup copies of the Operating Systems other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software.

Work with all reviewers to determine compliance with the backup policy.

This check does NOT apply to Compliance Validation Visits.

Fixes

EN230

The IAO will ensure all critical systems, to include infrastructure devices such as routers and inventory records, are backed up and copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocate

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN240 V0003998 CAT II Data backup is not properly performed.

8500.2 IA Control: CODB-3, CODB-2, CODB-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Data backup is not performed daily and recovery media is not stored offsite.

Checks

EN240

Interview the IAO to determine if there is a backup policy in place that ensures data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data.

CODB-3 Data Backup Procedures MAC I
Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

CODB-2 Data Back-up Procedures MAC II
Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and
confidentiality level.

CODB-1 Data Backup Procedures MAC III
Data backup is performed at least weekly.
This check does NOT apply to Compliance Validation Visits.

Work with the reviewers to determine compliance.

Fixes

EN240

The IAO will ensure data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

On-line backups to remote sites mee

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN250 V0003999 CAT II Ports and services are not blocked IAW policy.

8500.2 IA Control: ECSC-1

References: 8551.1 Ports, Protocols, and Services Management (PPSM) , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.7.13

Vulnerability The site has not blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Checks

EN250

Interview the IAO to determine if there is a procedure in place to identify needed ports and services allowed to traverse the Enclave boundary.

Work with the Network reviewer to determine compliance.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Fixes

EN250

The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Reference the Network Infrastructure STIG to o

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN260 V0004000 CAT I Perimeter Security is not in place.

8500.2 IA Control: ECSC-1, COEB-1, COEB-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran

Vulnerability Perimeter security is not in place at the Enclave network boundary. A firewall OR a router in deny-all posture is not in place.

Checks

EN260

EN260: Interview the IAO to determine if the site is aware of the DOD Defense in Depth strategy of Deny by Default on enclave perimeter devices.

The site will have either a Firewall OR a Router in a deny by default posture in order to satisfy this requirement. If the site does not have a firewall, they must have a deny all statement at the end of the router ACLs.

Work with the network reviewer to determine compliance.

Fixes

EN260

In accordance with the DOD philosophy of permit by exception, the NSO will ensure router ACLs or firewall rules are based on a policy of Deny-by-Default with blocks on all services and protocols not required by the site. Either a firewall or router with d

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN270 V0004001 CAT II Risk is not addressed for low assurance traffic.

8500.2 IA Control: DCPP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Low assurance/risky (red port) PPS traffic is allowed through a virtual private network (VPN) without addressing the risk to the other enclaves and is not approved by the DAA.

Checks

EN270

Work with the network reviewer to determine compliance. Interview the IAO to obtain DAA approval documentation.

Fixes

EN270

The IAO will ensure allowing Red port traffic through a VPN must address the risk to other enclaves and must be approved by the DAA.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN280 V0004002 CAT III No approval for exceptions to minimum requirements

8500.2 IA Control: DCBP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The DAA, Enclave Management Control Board (EMCB), or SIPRNet Program office has not approved exceptions to the Enclave STIG minimum requirements.

Checks

EN280

Work with all reviewers to determine compliance. Interview the IAO to determine EMCB, DAA, or SIPRNet PMO approval of exceptions.

Fixes

EN280

In order to comply with the enclave architecture as it pertains to LAN/WAN enclaves, the minimum requirements include the following devices or systems

- External Network Intrusion Detection System (IDS), anomaly detection, or prevention device if requi

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN290 V0004003 CAT II No external intrusion detection system (IDS).

8500.2 IA Control: EBBD-3, EBBD-2, EBBD-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability An external intrusion detection system (IDS) is not present at the enclave perimeter as directed by the Computer Network Defense Service Provider (CNDSP).

Checks

EN290

Work with the network reviewer to determine compliance. Interview the IAO to determine if required by CNDSP. If the site is unfamiliar with thier CNDSP, direct them to the DOD Directive O-8530.1 which requires a CNDSP.

Fixes

EN290

The IAM will ensure if directed by their CNDSP, the site will install and maintain an external NID at their enclave perimeter.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN300 V0004004 CAT II The external NID is not under CNDSP control.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The external NID is not under the operational control of the CNDSP and is not located outside of a local firewall.

Checks

EN300

Interview the IAO to determine if there is an agreement with the CNDSP to perform configuration management and maintain administrative control of the external IDS.

Work with the network reviewer to determine if the location of the External NID is in compliance.

Fixes

EN300

The Enclave Perimeter network IDS will be under the operational control and configuration management of the appropriate CNDSP. The Enclave NID will be positioned outside of any local firewalls so that the CNDSP has visibility of all attempted malicious a

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN310 V0004005 CAT III GNC has not approved requirement JID.

8500.2 IA Control: DCBP-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The GNC has not reviewed and approved requirements for enclave perimeter Joint Intrusion Detection System (JID) to ensure integration with the Sensor Grid.

Checks

EN310

The responsible party for this check is the GNC. The GNC along with the CNDSP is responsible for determining if the installation of a JID meets the requirements of integration with the sensor grid.

Fixes

EN310

The GNC will review and approve requirements for enclave perimeter Joint Intrusion Detection System (JID) to ensure integration with the Sensor Grid.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN320 V0004006 CAT II Routers not in compliance with the Network STIG.

8500.2 IA Control: ECSC-1, DCBP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The NSO will ensure routers are configured in accordance with the Network Infrastructure STIG.

Checks

EN320

Interview the IAO to determine if there is a process/procedure for following and adhering to the security guidance in the Network Infrastructure STIG.

Work with the Network reviewer to determine compliance.

Fixes

EN320

The NSO will ensure that the routers are configured in accordance to the security guidance established in the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN330 V0004007 CAT II Egress/ Ingress filtering is not in compliance.

8500.2 IA Control: DCPP-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Egress and Ingress filtering is not in compliance with the Network Infrastructure STIG.

Checks

EN330

Interview the NSO to determine if the there is a process and procedure to identify all necessary ports traversing the enclave boundary. Egress filtering rules are applied denying all outbound traffic with illegitimate (i.e., not local network) IP addresses and both ingress and egress filtering rules are applied denying all Distributed Denial of Service (DDOS) ports and IPs in accordance with the Network Infrastructure STIG.

Work with the Network Reviewer to determine compliance.

Fixes

EN330

The NSO will ensure egress filtering rules are applied denying all outbound traffic with illegitimate (i.e., not local network) IP addresses and both ingress and egress filtering rules are applied denying all Distributed Denial of Service (DDOS) ports and

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN340 V0004008 CAT II Network perimeter devices not STIG compliant.

8500.2 IA Control: ECSC-1, DCPP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Enclave firewalls and routers are not configured with the most restrictive security rules possible and in accordance with the Network Infrastructure STIG. The organization's SSAA is not updated to reflect the firewall and router installation.

Checks

EN340

Interview the IAO to determine if the SSAA is up to date with complete and accurate perimeter defense (firewall and router) information.

Work with the Network reviewer to determine whether or not the network devices are in compliance with Network Infrastructure policy.

This finding can be closed if all open vulnerabilities are addressed with a POA&M and the remainder are in a fixed or not a finding status.

Fixes

EN340

The NSO will ensure enclave firewalls are configured with the most restrictive security rules possible ("that which is not expressly allowed is denied") (Deny by Default). A Firewall Implementation Description Report is developed and maintained for each

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN350 V0004009 CAT II The firewall does not meet requirements.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran

Vulnerability The firewall does not meet the requirements set forth in the CJCSM 6510.01 and the Network Infrastructure STIG

Checks

EN350

Work with the Network Reviewer to determine compliance. Enclosure C, Appendix K details the CJCSM 6510.01 firewall requirements.

Fixes

EN350

The IAO will ensure only COTS firewall products that meet the criteria set forth in the Network Infrastructure STIG and the CJCSM 6510.01 will be employed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN360 V0004010 CAT III No documentation for permitted IPs.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Permitted IPs and ports, protocols and services are not documented.

Checks

EN360

Interview the NSO to determine if all IPs, ports, protocols, and services are documented.

Fixes

EN360

The IAO will ensure all permitted IPs and PPSs are documented.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN370 V0004011 CAT I Unapproved connections are present.

8500.2 IA Control: EBBD-1, EBBD-3, EBBD-2, EBPW-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Direct network connections between DOD managed networks and the Internet, NIPRNet, SIPRNet, or other external networks exist and there is no DOD approved waiver for the connection.

Checks

EN370

Interview the IAO to determine if direct network connections between managed networks and the Internet, NIPRNet, SIPRNet, or other external networks exist. Ask to see the DOD approved waiver for the connection.

Work with the Network reviewer to determine compliance.

Fixes

EN370

The IAO will ensure direct network connections between managed networks and the Internet, NIPRNet, SIPRNet, or other external networks do not exist if there is no DOD approved waiver for the connection.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN390 V0004012 CAT II VPN implementations are not in compliance.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability VPN implementations are not in compliance with the Network Infrastructure STIG.

Checks

EN390

Work with the Network Reviewer to determine compliance.

Fixes

EN390

The NSO will ensure all VPN implementations adhere to the VPN section of the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN400 V0004013 CAT II VPNs are configured as split tunnel.

8500.2 IA Control: ECSC-1, EBVC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability VPNs are not established as a full tunnel (non-split tunnel) and/or do not terminate outside of the firewall.

Checks

EN400

Work with the Network reviewer to determine compliance.

Fixes

EN400

The NSO will ensure VPNs are established as a full tunnel and VPNs will terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router). Location is not as paramount as being in compliance w

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN410 V0004014 CAT II FIPS 140-2 encryption algorithm is not used.

8500.2 IA Control: ECNK-1, ECCT-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 3.2.4.3.3, 3.2.4.3.2, and 3.2.4.3.4, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability An approved FIPS 140-2 encryption algorithm is not used for VPN communications to/from the network.

Checks

EN410

interview the IAO to determine if there is a procedure/policy in place to ensure that all encrypted traffic, to include VPNs, uses only FIPS 140-2 compliant algorithms.

Work with the Network reviewer to determine compliance.

Fixes

EN410

The NSO will ensure all VPN communications to/from the network employ at a minimum a FIPS 140-2 approved data encryption algorithm (i.e., Advanced Encryption Standard (AES) or Triple-Data Encryption Standard [3DES]). (See http://csrc.nist.gov/cryptval.)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN420 V0004015 CAT II VPN traffic is not visible to an IDS.

8500.2 IA Control: EBVC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability VPN traffic is not visible to an IDS.

Checks

EN370

Work with the Network reviewer to determine compliance.

Fixes

EN370

The NSO will ensure that at a minimum, all VPN solutions include an IDS capability on the unencrypted portion of the network or system. DODI 8500.2 IA Control EBVC-1 requires that all VPN traffic is visible to a Network IDS.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN430 V0004016 CAT II The DNS architecture is not in compliance.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , DNS STIG

Vulnerability The DNS server and architecture is not configured in accordance with the DNS STIG.

Checks

EN430

Work with the DNS reviewer to determine compliance.

Fixes

EN430

The IAO will ensure that the DNS server and architecture are configured in accordance with the DNS STIG.

All vulnerabilities will be closed or addressed with a POA&M to close this finding.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN440 V0004017 CAT I Privileged level remote access is not encrypted.

8500.2 IA Control: EBRP-1, EBRU-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Privileged level user remote access is not encrypted.

Checks

EN440

Interview the IAO to determine that a policy is in place to prohibit privileged level access without encryption.

Work with the reviewers to determine compliance.

Fixes

EN440

The IAO will ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption (FIPS 140-2 validated or Type 1), to secure the data traversing the network.

EBRP-1: Remote access for privileged functions is

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN450 V0004018 CAT II Remote access traffic/data bypasses security.

8500.2 IA Control: EBRU-1, EBRP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Remote access traffic/data bypasses the security architecture of the enclave.

Checks

EN450

Work with the Network reviewer to determine if remote access to the network is in compliance with requirements. Work with all reviewers to determine if remote access to their systems is controlled in accordance with Network requirements.

Fixes

EN450

The NSO will ensure remote access device traffic/data does not bypass the security architecture as outlined in the Network Infrastructure STIG (i.e., all ingress traffic passes through the firewall and NIDS).

EBRU-1: All remote access to DoD informati

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN460 V0004019 CAT III Content security checking is not employed.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Content security checking is not employed for email, ftp or http data.

Checks

EN460

Interview the IAO to determine if policy is in place to ensure all networks employ Content Security checking mechanisms for e-mail with attachments, ftp data, and http data. Products from the DOD standard anti-virus contract should be used if available.

The available list of attachments to be blocked via email systems is located at www.nsa.gov under Information Assurance, Supporting Documents, "Outlook Email Security in the Midst of Malicious Code Attacks".

Fixes

EN460

The IAO will ensure all networks employ Content Security Checking, mechanisms for e-mail with attachments, ftp data, and http data. Products from the DOD standard anti-virus contract should be used.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN470 V0004020 CAT I Anti-virus software not installed or out of date.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Anti-virus software is not installed or the signatures are not downloaded and up to date.

Checks

EN470

Interview the IAO to determine if there is a policy and a process in place to install anti-virus software and maintain virus signatures updates on all devices.

Work with the reviewers to determine compliance.

Fixes

EN470

The IAO will ensure anti-virus software is installed and updated virus detection signatures are downloaded and installed at least every 14 days or when the JTF provides an update.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN480 V0004021 CAT II A DMZ is not established.

8500.2 IA Control: EBBD-3, EBBD-1, EBPW-1, EBBD-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A DMZ is not established within the Enclave Security Architecture to host any remotely accessible system.

Checks

EN480

Interview the IAO to determine if there is a policy in place to identify all remotely accessible systems and place them in a DMZ.

Fixes

EN480

The IAO will ensure that a DMZ is established within the Enclave security architecture to host any publicly accessible system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN490 V0004022 CAT II The DMZ is not a screened subnet.

8500.2 IA Control: EBBD-3, EBBD-1, EBBD-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The DMZ is not located between the firewall and the router or on a dedicated network segment.

Checks

EN490

Work with the Network reviewer to determine compliance.

Fixes

EN490

The IAO will ensure the DMZ is located on the network segment connecting the firewall to the border router or on a dedicated network segment connected to the firewall.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN500 V0004023 CAT III Operating systems without appropriate EAL.

8500.2 IA Control: DCAS-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Operating systems without an EAL rating of 4 or higher are being used without mission justification.

Checks

EN500

Interview the IAO to ensure that the purchase or use of operating systems is in compliance with the requirement for EAL 4 evaluation.

Fixes

The IAO will ensure enclaves u

The IAO will ensure enclaves use only OSs with an EAL4 or higher rating. OSs that do not contain EAL4 level security features will not be used unless justified by a mission requirement and approved by the EMCB. An example of such a mission requirement w

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN510 V0004024 CAT II Operating systems are not in compliance.

8500.2 IA Control: DCCS-2, DCCS-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Operating systems are not in compliance with the applicable OS STIG.

Checks

EN510

Work with the OS reviewers to determine compliance with this requirement. Interview the IAO to determine if a process is in place to configure all operating systems in accordance with the applicable security guidelines (e.g. STIG). Ensure a POA&M is in place for all outstanding open vulnerabilities.

Fixes

EN510

The IAO will ensure host OSs are configured according to the latest applicable STIG. STIGs provide configuration guidance to achieve an optimal level of security. Operational requirements may prevent implementation of all STIG requirements. In these ca

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN520 V0004025 CAT IV Failure to follow configuration guidance.

8500.2 IA Control: ECSC-1, DCCS-2, DCCS-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Major new device configuration or operating systems changes are installed without security guidance.

Checks

EN520

Work with the reviewers to determine compliance. Interview the IAO to determine if there is a process in place to prohibit new major OS changes or device configuration changes until security guidance is available.

Fixes

EN520

The IAO will ensure major new OS changes or device configuration changes are not installed until security guidance is published unless approved by the appropriate DAA. The DAA responds to a request for approval within three months. While guidance is bei

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN530 V0004026 CAT III The SSAA is not complete.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.7.5 and 5.9.3, Department of Defense (DOD) Directive 8500.1, Information Assurance Para. 4.1.3

Vulnerability The SSAA does not include the OS security requirements contained in the Enclave STIG.

Checks

EN530

Review the SSAA to determine if the operating system requirements contained in the STIG are incorporated into the System Architectural Description" and the "Security Requirements and/or Requirements Traceability Matrix."

Fixes

EN530

The IAO will ensure while following the procedures outlined in the DITSCAP, each SSAA includes the OS security requirements in this section as part of the "System Architectural Description" and the "Security Requirements and/or Requirements Traceability M

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN540 V0004027 CAT II Servers do not employ HIDs.

8500.2 IA Control: ECID-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Servers do not employ Host Based Intrusion Detection (HIDS).

Checks

EN540

Interview the IAO to determine if there is a process and policy in place to ensure Host Based IDS is installed on all servers.

Work with the reviewers to determine compliance.

Fixes

EN540

The IAO will ensure all servers employ HIDS, if technically feasible. This requirement may not pertain to legacy systems and cutting edge devices that do not yet have the capability. Documentation must exist from the vendor to approve any variance from

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN550 V0004122 CAT III HID alarms are ignored.

8500.2 IA Control: ECID-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The SA is not responding to initial real time HIDs alarms and do not perform analysis of reports.

Checks

EN550

Interview the IAO to determine if there is a policy in place to to determine administrator responsibilities for Host Based Intrusion Detection response and retrospective analysis of reports.

Fixes

EN550

The IAO will ensure the SA is responsible for initial response to real-time alarms and perform retrospective analysis of reports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN560 V0004123 CAT II No HIDs event reporting procedures.

8500.2 IA Control: VIIR-2, ECAT-2, ECAT-1, VIIR-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Significant Host Based IDS events are not reported to the sites Computer Network Defense Service Provider (CNDSP).

Checks

EN560

Interview the IAO to determine if there is a procedure in place to report any suspicious activity to the site's CNDSP. Ask to see the Incident Response procedures and ensure that they are being followed.

Fixes

EN560

The IAO will ensure significant incidents are reported to the site's CNDSP.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN570 V0004124 CAT I Content security mechanisms are not deployed.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Servers and/or workstations do not employ content security mechanisms from the DOD anti-virus contract.

Checks

EN570

Interview the IAO to determine if there is a policy/procedure in place to ensure all workstations and servers delpoy content security mechanisms.

Work with the review team to determine compliance for all servers and workstations.

Content Security Checking can also be provided at the host level. In many situations, full content checking at the enclave level may not be possible due to VPN or application layer encryption. In addition, only system-based Content Security Checking can be used to protect workstations from malicious programs that are imported on floppy disks, CD ROMs, Zip drives, tapes, or other removable media.

Fixes

EN570

The IAO will ensure all workstations and servers employ Content Security Checking mechanisms from the DOD-wide anti-virus contract.

Content Security Checking can also be provided at the host level. In many situations, full content checking at the encl

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN580 V0004125 CAT II Content security mechanism not compliant.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Content security mechanism is not configured to scan all files upon access.

Checks

EN580

Interview the IAO to determine if there is a policy in place to ensure that antivirus software is configured to run in back-ground mode and scan all files upon access.

Work with the reviewers to determine compliance.

Fixes

EN580

The IAO will ensure Content Security Checking mechanisms are configured to run in a background mode and scan files upon access

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN590 V0004126 CAT I Virus detection signatures are out of date.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Virus detection signatures are not downloaded and installed at least every 14 days.

Checks

EN560

Interview the IAO to determine if there is a policy/procedure in place to update antivirus signatures at least every 14 days.

Work with the reviewers to determine compliance.

Fixes

The IAO will ensure updated vi

The IAO will ensure updated virus detection signatures are downloaded and installed, at least every 14 days.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN600 V0004127 CAT IV DOD home users are not using anti-virus.

8500.2 IA Control: ECVP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The site does not encourage employees to use the DOD anti-virus software on their home computers.

Checks

EN600

Interview the IAO and ask to see the remote access or Telework policy and ensure that it includes the requirement to provide DOD employees access to anti-virus software.

Fixes

EN600

The IAM will ensure their organization strongly encourages DOD employees to install the DOD-licensed anti-virus software on the employees' home computers. Organizations should publicize that this software is available free for home use by DOD employees.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN610 V0004128 CAT III Local policies do not exist for Internet posting.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Local policies have not been developed to ensure information posted to the Internet/Intranet is reviewed by a duly appointed PAO or authorized content reviewer for sensitive information.

Checks

EN610

Interview the IAO to determine compliance and ask to see the policy on posting DOD information to a website.

Fixes

EN610

The IAO will verify that local policies are developed to ensure all originated information posted to the Internet and/or Intranet (i.e., public web servers) is reviewed for sensitive content and approved for use by the PAO or authorized appointed content

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN620 V0004129 CAT II Non-compliant web servers.

8500.2 IA Control: ECSC-1, DCCS-2, DCCS-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The web servers are not configured in accordance with the Web Server STIG.

Checks

EN620

Work with the Web reviewer to determine compliance.
All vulnerabilities will be closed or addressed with a POA&M to close this finding.

Fixes

EN620

The IAO will ensure all web servers are configured in compliance with the latest Web Server STIG. If operational requirements prevent implementation of all STIG requirements, formal exceptions require DAA approval and a POA&M.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN630 V0004130 CAT II Port redirection is in use.

8500.2 IA Control: ECSC-1

References: 8551.1 Ports, Protocols, and Services Management (PPSM) , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Non-standard ports or port redirection is used for web services.

Checks

EN630

Work with the Web and Network reviewer to determine compliance.

Fixes

EN630

The IAO will ensure only standard ports are used in accordance with the DOD PPS CAL and the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN640 V0004131 CAT III Public web server location s is not compliant.

8500.2 IA Control: DCPA-1, EBPW-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Web servers are not isolated in a DMZ or separate LAN segment.

Checks

EN640

Work with the web and network reviewer to determine compliance.

Fixes

EN640

The IAO will ensure Public Web servers, approved by the Public Affairs Office (PAO), are isolated on a separate LAN segment (DMZ) from all private DOD systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN650 V0004132 CAT II Web servers are not protected.

8500.2 IA Control: EBRP-1, EBRU-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Web servers are not protected from unauthorized remote access.

Checks

EN650

Work with all reviewers to determine compliance: Network, Web, and OS.

Fixes

EN650

The IAO will ensure web servers are protected from unauthorized remote access at the enclave perimeter and host levels.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN660 V0004133 CAT II 128 bit SSL and DOD PKI are not utilized.

8500.2 IA Control: DCBP-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability 128 bit SSL and DOD PKI are not utilized for web services.

Checks

EN660

Work with the Web reviewer to determine compliance.

Fixes

EN660

The IAO will ensure all Internet applications providing encryption, use at a minimum 128-bit SSL encryption and utilize DOD Public Key Infrastructure (PKI) certificates for authentication if technically feasible. (See Table 3-1 in the Enclave STIG for en

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN670 V0004134 CAT I Information is transmitted incorrectly.

8500.2 IA Control: ECSC-1, ECCT-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Classified or sensitive information is transmitted over unapproved communications systems or non-DOD systems.

Checks

EN670

Interview the IAO and determine if there is a Classified or Sensitive Handling/transmitting policy in place to include email, Instant Messaging and Weblogs (BLOG).

Fixes

EN670

The IAO will ensure classified information is not transmitted over any communications system unless it is transmitted using approved NSA security devices in addition to approved security procedures and practices.

Government-owned, Defense Message Syste

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN680 V0004135 CAT I Anonymous mail redirection/relay is not blocked.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Anonymous mail redirection/relay is not blocked.

Checks

EN680

Work with the OS reviewer/email server reviewer to determine compliance.

Fixes

EN680

The IAO will ensure all mail connections to and from mail servers used for anonymous mail redirection are blocked. Mail should be traceable to an individual and known servers. Any servers that have the capability for anonymous mail redirection pose a th

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN690 V0004136 CAT II Malicious mail attachments are not blocked.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Mail attachments are not blocked in accordance with the Network Infrastructure STIG, the NSA Guide to E-mail Security in the Wake of Recent Malicious Code Incidents, and the NSA E-mail and Executable Content Guides.

Checks

EN690

Work with the Network Reviewer to determine compliance and interview the IAO to determine if they are aware of the NSA Guidelines on email attachment blocking.

Fixes

EN690

The IAO will ensure all mail systems are configured to block attachments in accordance with the Network Infrastructure STIG, the NSA Guide to E-mail Security in the Wake of Recent Malicious Code Incidents, and the NSA E-mail and Executable Content Guides.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN700 V0004137 CAT I Unsigned Category 1 mobile code not blocked.

8500.2 IA Control: DCMC-1, ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Unsigned or untrusted Category 1 and non-categorized mobile code is not blocked at the enclave perimeter.

Checks

EN700

Interview the IAO to determine if the site has a policy in place to block unsigned mobile code, unless signed from a trusted source, at the Enclave perimeter.

Fixes

EN700

The IAO will ensure Category 1 and non-categorized mobile code is blocked at the enclave perimeter unless signed from a trusted source and approved.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN710 V0004138 CAT II DOD policy on mobile code is not being followed.

8500.2 IA Control: DCMC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability DOD policy on mobile code is not being followed.

Checks

EN710

Interview the IAO to ensure familiarity with DOD Mobile Code policy and implementation.

Determine moblie code compliance with results obtained from Application, Web, and Desktop reviewers.

Fixes

EN710

The IAO will ensure the DODI 8550.cc, Use of Mobile Code Technologies in DOD Information Systems, is adhered to.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN730 V0004139 CAT II Non-Compliant database.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Database Security Technical Implementation Guide

Vulnerability The Database Management System (DBMS) is not secured in accordance with the Database STIG.

Checks

EN730

Work with the Database reviewer to determine compliance.

All vulnerabilities will be closed or addressed with a POA&M to close this finding.

Fixes

EN730

The IAO will ensure all DBMSs are configured in compliance with the latest Database STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN735 V0004756 CAT II Wireless LANs and/or devices are not compliant.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , Wireless STIG

Vulnerability Wireless Local Area Networks (LANS) and/or devices are not secured in accordance with the Wireless STIG.

Checks

EN735

Work with the Wireless reviewer to determine compliance.

All vulnerabilities will be closed or addressed with a POA&M to close this finding.

Fixes

EN735

The IAO will ensure wireless LANs and devices are configured in accordance with the Wireless STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN740 V0004140 CAT II WEP is the only form of encryption used.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , DODD 8100.2 Use of Commercial Wireless Devices, Se , Wireless STIG

Vulnerability WEP is the only form of encryption on a wireless network.

Checks

EN740

Work with either the Network or Wireless reviewer to determine compliance.

Fixes

EN740

The IAO will ensure that additional encryption, beyond WEP, will be employed, such as encrypted VPN, SSL, or SSH.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN750 V0004141 CAT III Services not required are enabled.

8500.2 IA Control: ECSC-1

References: Wireless STIG , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Services not required are enabled on wireless devices.

Checks

EN750

Work with the Wireless reviewer to determine compliance.

Fixes

EN740

The IAO will ensure all services not needed for operational use are disabled on wireless clients.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN760 V0004142 CAT I Wireless devices or connections not approved.

8500.2 IA Control: ECSC-1

References: Wireless STIG , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Users install wireless hardware or software or alter the configuration without DAA approval.

Checks

EN760

Work with the wireless reviewer to determine if there are wireless devices. Interview the IAM/IAO to determine if there is DAA approval for any wireless device or connection.

All vulnerabilities will be closed or addressed with a POA&M to close this finding.

Fixes

EN760

The IAO will ensure a user/administrator does not install wireless hardware or software or otherwise alter the configuration on government-controlled devices for connecting to a wireless network without DAA approval. The use of Wireless devices requires D

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN770 V0004143 CAT I Personal wireless devices used for remote access.

8500.2 IA Control: ECWN-1

References: Wireless STIG , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Personally owned wireless devices (non-GFE) are used for remote access to Government systems or networks.

Checks

EN770

Interview the IAO to determine compliance and ask to see the Wireless usage policy.

Fixes

EN770

The IAO will ensure personally owned wireless devices are not used for remote access to Government systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN780 V0004144 CAT I Non SecNet 11 devices on the SIPRNET.

8500.2 IA Control: ECSC-1, ECWN-1

References: DODD 8100.2 Use of Commercial Wireless Devices, Se , Wireless STIG , ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Non SecNet 11 devices have been identified on the SIPRNet.

Checks

EN780

Work with the Network and Wireless reviewer to determine compliance.

Fixes

EN780

The only approved wireless technology for the SIPRNET is SecNet-11.

The IAO will ensure that the DAA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data, including the SecNet 11. (Refe

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN785 V0007549 CAT II No wireless discovery policy.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A policy is not defined or implemented for scanning for rogue wireless devices.

Checks

EN785

Interview the IAO to determine if a policy is in place to scan for wireless devices throughout the enclave.

Fixes

EN785

The IAO will ensure a policy is in place to periodically scan for rogue wireless devices.

Refer to the Wireless STIG and the DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG),

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN785 V0007571 CAT III No policy to scan for wireless devices.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A policy is not defined or implemented for scanning for rogue wireless devices.

Checks

EN785

Interview the IAO to determine if a policy is in place to scan for wireless devices throughout the enclave.

Fixes

EN785

The IAO will ensure a policy is in place to periodically scan for rogue wireless devices.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN790 V0004145 CAT II Online automated vulnerability tools are not used.

8500.2 IA Control: ECMT-1, VIVM-1, ECMT-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Online automated vulnerability tools are not operated and maintained in accordance with JTF CTO 05-19.

Checks

EN790

In order to be compliant with this check the following must apply:

1. Scans must be run monthly.

2. Components must implement Secure Configuration
Compliance Verification Initiative (SCCVI) and Secure Configuration Remediation Initiative (SCRI), or similar tools, on all DOD networks.

3. If using the recommended SCCVI tool, ensure vulnerability scans are conducted with:
a. Domain Admin account to each domain or local machine to be scanned. This can be a specific account created just for the scans or a site-used domain admin account. Verify through Credentials management in the SCCVI tool.

(If not using SCCVI, ensure the tool is being run with the appropriate settings necessary to complete a proper scan.)

b. Server service and Remote Registry turned on at every target.
c. Account lockout policies in place prior to scanning and only during the duration of the scan.
d. Anti-virus and personal firewalls disabled on scanning machine.
e. All Audits auditing group is used.

4. Verify Simple File Sharing is disabled on Windows XP systems

5. Verify IP range.
a. Verify entire IP range(s) is being scanned (NIPRNet and SIPRNet). Work with network adminstrator and/or IAM, using network diagram, router configurations, etc.
b. Verify IP range(s) are being scanned for importing into VMS based on varying criteria, such as "Managed By", Program of Record (POR), Area of Responsibility (AOR), and/or specific network ranges (workstations, domain controllers, network devices, etc.).
c. Verify each scan job is named according to the IP range(s) being scanned (i.e., job name DMS contains IP range of the DMS systems only).

6. Verify in VMS:
a. Do asset buckets exist?
b. Are the asset buckets constructed based on varying criteria (see 4b)?
c. If not, assist site in creating their asset buckets as they pertain to their network scan structure (see 5b).

Fixes

EN790

The IAO will ensure the SAs operate and maintain online automated vulnerability assessment tools for each system on their network, including systems managed remotely by other organizations. The IAO will ensure the output of these tools is reviewed at lea

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN800 V0004146 CAT III No coordination for site access for the SCAO.

8500.2 IA Control: VIVM-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Para. 5.7.1.6, ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The site does not coordinate access for the SIPRNet PM to perform random assessments within the Enclave.

Checks

EN800

Interview the IAO to determine if the site is coordinating scan or assessment efforts with the SIPRNet Program Management office.

Fixes

EN800

Random assessments across the SIPRNet will be performed by the SIPRNet Program Management office, and network managers will coordinate with them for access into the Enclave.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN805 V0004755 CAT II Non-compliant Application infrastructure.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The application infrastructure is not in compliance with the Application Security Checklist.

Checks

EN805

Work with the Application reviewer to determine compliance.
All vulnerabilities will be closed or addressed with a POA&M to close this finding.

Fixes

EN805

The IAO will ensure that the application infrastructure is in compliance with the Application Security Checklist.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN810 V0004147 CAT III Application developers use unapproved PPS.

8500.2 IA Control: DCPP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , 8551.1 Ports, Protocols, and Services Management (PPSM)

Vulnerability Application developers use unapproved ports, protocols or services.

Checks

EN810

Interview the IAO to determine if there is a process in place for all application developers to register the ports, protocols, and services used in any new application being developed. Ensure that the application is using approved ports, protocols, and services as defined by the DOD 8551.1 and the PPS Assurance Category Assignments list.

Work with the Application reviewer to determine compliance.

Fixes

EN810

The application developer will ensure that only ports, protocols, and services approved by the DOD Ports, Protocols, and Services Assurance Category Assignments List are used during application development. Any other PPS's that are written into the appli

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN820 V0004148 CAT III Application developer did not submit new ports.

8500.2 IA Control: DCPP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , 8551.1 Ports, Protocols, and Services Management (PPSM)

Vulnerability The application developer did not submit new ports or protocols to the appropriate approving authority which in turn are submitted through the PPSM process in accordance with DOD 8551.1.

Checks

EN820

Interview the IAO to determine if there is a process in place for all application developers to register any new ports, protocols, and services used in any application being developed.

Work with the Application reviewer to determine compliance.

Fixes

EN820

The application developer will ensure that applications that use new protocols or ports are submitted to the appropriate approving authority for that organization, which in turn will be submitted through the PPMP.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN830 V0004149 CAT III Static port allocation is not used on servers.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Application developers use random ports or non-fixed port numbers on servers.

Checks

EN830

Interview the IAO to determine if there is policy in place to prohibit application developers from using random ports and instead use static port allocation when developing new applications.

Work with the application reviewer to determine compliance.

Fixes

EN830

The application developer will ensure that protocols do not use random ports or non-fixed port numbers on servers. Instead, static port allocation should be used to avoid proliferation of possible vulnerabilities.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN840 V0004150 CAT III IP Services have been modified.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability IP services have been modified during application development and the application is no longer compliant with the relevant Request For Comments (RFC) standard.

Checks

EN840

Interview the IAO to determine if there is policy in place to prohibit application developers from modifying IP services or rendering the services non-compliant with RFC standards.

Fixes

EN840

The application developer will not modify any IP services and will ensure that each application is compliant to the relevant Request For Comments (RFC) standard.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN850 V0004151 CAT III IP services have been modified or are not in compl

8500.2 IA Control:

References:

Vulnerability IP services have been modified or are not in compliance with an RFC.

Checks

Fixes

The application developer will

The application developer will not modify any IP services and will ensure they are compliant with an associated Request For Comments (RFC) standard.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN860 V0004152 CAT II Code has been written that requires a client to pe

8500.2 IA Control:

References:

Vulnerability Code has been written that requires a client to perform IP forwarding.

Checks

Fixes

The application developer will

The application developer will not write code that requires clients to perform IP forwarding.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN865 V0007550 CAT II Port security solution is not in place.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A port security solution is not in place to protect the network.

Checks

EN865

Interview the IAO to determine if a policy is in place to require port security for the network. Work with the Network reviewer to determine compliance.

Fixes

EN865

The IAO will ensure a port security solution is in place to protect access to the network.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN870 V0007683 CAT II HIDS not employed on the device.

8500.2 IA Control: ECID-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Encryption protocols such as SSL and SSH transmit traffic directly to the host, and a host based intrusion detection (HID) system is not employed on the device.

Checks

EN870

Work with the reviewers to determine if HIDs are employed on host systems.

Verify with the IAO that there is a policy in place to ensure HIDs are deployed.

Fixes

EN870

The IAO will ensure if encryption protocols such as SSL and SSH transmit traffic directly to the host, a host based intrusion detection (HID) system is employed on the device if supported.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN880 V0007684 CAT II VPN bypasses IDS visibility.

8500.2 IA Control: EBVC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Network traffic is not visible to an Intrusion Detection System or VPN traffic bypasses the security architecture.

Checks

EN880

Work with the Network and OS reviewers to determine compliance.

Fixes

EN880

The IAO will ensure all network traffic is visible to an Intrusion Detection System (IDS). VPN traffic does not bypass the security architecture and must terminate in order for the traffic to be processed by a network IDS (NID) or Host Based IDS (HID).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN890 V0008259 CAT I Unencrypted FTP and/or Telnet.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability FTP and/or telnet from outside the enclave into the enclave is permitted, without applying the following conditions:

- FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network (VPN). The connection will te

Checks

EN890

FTP and telnet are permissible inside an enclave, behind the premise router and protected by a firewall and router access control lists (ACLs); however, the requirement must be documented and maintained by the Information Assurance Officer (IAO). If either of these services is not required, the service will be deleted, disabled, or turned off. If the service is disabled or turned off, the site will continue to ensure that all appropriate patches are applied. When used, all associated traffic will be restricted by IP source and destination address if technically feasible, and other mitigating controls as required by the appropriate STIG will be enforced.

If FTP or Telnet is allowed through the Enclave boundary unencrypted, this is a finding.

Work with the reviewers to determine compliance.

Fixes

EN890

The IAO will ensure FTP and telnet from outside the enclave into the enclave is not permitted, unless encrypted and the following conditions apply:

- FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN900 V0008260 CAT II FTP UserIDs are not changed every 90 days.

8500.2 IA Control: IAIA-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability FTP UserIDs passwords do not expire or are not changed within 90 days.

Checks

EN900

Work with the applicaiton and/or OS reviewer to determine compliance.

Fixes

EN900

The IAO will ensure all user FTP UID passwords have an expiration date and the password is changed every 90 days.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN910 V0008353 CAT I FTP UID has administrative privileges.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability FTP or Telnet is used with a userid (UID)/password that has administrative or root privileges.

Checks

EN910

Work with the reviewers to ensure under no circumstances are FTP or telnet used with a userid (UID)/password that has administrative or root privileges.

Fixes

EN910

The IAO will ensure under no circumstances are FTP or telnet used with a userid (UID)/password that has administrative or root privileges.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

EN920 V0008354 CAT II Anonymous FTP within the enclave.

8500.2 IA Control: IAIA-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability An “anonymous” FTP connection within the enclave is established.

Checks

EN920

Interview the IAO to determine if there is a policy in place to prohibit “anonymous” FTP connection within the enclave.

Work with the reviewers to determine compliance.

Fixes

EN920

The IAO will ensure an “anonymous” FTP connection within the enclave is not allowed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

ENTD100 V0003918 CAT II Test and development systems are not isolated.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Test and development systems are not connected to an isolated network separated from production systems.

Checks

ENTD100

Interview the IAO to determine if they have a policy in place that isolates test and development traffic and/or testing from production systems. Network reviewer to validate based on network diagrams.

Fixes

ENTD100

The IAO will ensure that all systems supporting application development, software testing, and OS maintenance are connected to an isolated network separated from production systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

ENTD110 V0003919 CAT II Out of band access is not utilized for T&D.

8500.2 IA Control: ECSC-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Out of band access is not utilized to access a test and development enclave.

Checks

ENTD110

Interview the IAO to determine if they have a policy in place that requires the use of out-of-band methods to access a Test and Development network from outside of the enclave. Coordinate this response with the Network reviewer.

Fixes

ENTD110

The IAO will ensure that out-of-band access is utilized if outside access to the test and development systems is required

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes: